PCT/DE 97 / 05081

# BUNDESREPUBLIK DEUTSCHLAND



## Bescheinigung



Die Deutsche Telekom AG in Bonn/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren zur Übertragung von Signalen"

am 1. Oktober 1996 beim Deutschen Patentamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patentamt vorläufig die Symbole H 04 L, H 04 K und H 04 N der Internationalen Patentklassifikation erhalten.

München, den 17. Juni 1997

**Der Präsident des Deutschen Patentamts**

Im Auftrag

Wehner

Aktenzeichen: 196 40 526.2

# B E S C H R E I B U N G

## VERFAHREN ZUR ÜBERTRAGUNG VON SIGNALEN

Die Erfindung betrifft ein Verfahren zur Übertragung von Signalen nach dem Oberbegriff des Patentanspruchs 1.

Bei der Übertragung von Signalfolgen spielt die authentische Übertragung der Daten bzw. Signale immer eine größere Rolle. So ist zum Beispiel in ISO/IEC 9797, Information technology - Security techniques - Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm (JTC1/SC27 1994) eine Lösung für dieses Problem beschrieben. Dabei sind dem Sender und dem Empfänger gleiche geheime Schlüssel in Verbindung mit einem Verschlüsselungsalgorithmus (block cipher, encipherment algorithm) oder mit einer schlüsselabhängigen Einwegfunktion (crypthgraphic check function) zugeordnet. Dies kann zum Beispiel auf einer Chipkarte erfolgen. Der Sender fügt jedem Signal (Datum) eine kryptgraphische Prüfsumme (Message authentication code) hinzu, die vom geheimen Schlüssel und dem kryptographischen Algorithmus (Verschlüsselung bzw. Einwegfunktion) abhängt. Der Empfänger berechnet seinerseits die Prüfsumme und erkennt die empfangenen Signale bei Gleichheit der Prüfsumme als authentisch an. Diese Lösung hat jedoch folgende Nachteile: Um eine Änderung der Reihenfolge der übertragenen Daten zu erkennen, wird die Prüfsumme eines Signals abhängig von der Prüfsumme der bisher gesendeten Signale berechnet. Auch für den Fall, daß nach jedem Signal eine Prüfsumme gesendet wird, ist dies notwendig, da sonst ein Angreifer Signalprüfsummenpaare aufzeichnen und in geänderter Reihenfolge unbemerkt einspielen könnte. Dies erfordert in der bekannten Lösung für jede Prüfsumme eine Durchführung des kryptographischen Algorithmus. Da Reihenfolge und

Auswahl der Signale nicht genau im Voraus feststehen, ist es auch nicht möglich, die erforderlichen Prüfsummen im Voraus zu berechnen.

In einer zeitkritischen Umgebung kann dies zu Problemen führen. Die Berechnung des kryptographischen Algorithmus kann zum Beispiel auf einer Chipkarte stattfinden. Beim Einsatz einer schon evaluierten Chipkarte ist dies vorteilhaft, ansonsten ist eine zusätzliche Softwareimplementierung des Algorithmus erneut zu evaluieren. Die Kommunikation mit der Chipkarte und die Berechnung des kryptographischen Algorithmus auf der Chipkarte sind sehr zeitintensiv.

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren zur authentischen Signal- bzw. Datenübertragung zu schaffen, das zu einem vorgegebenen Signalvorrat und einer vorgegebenen maximalen Anzahl zu übertragender Signale die Berechnung von Authentifikationsformationen vorab ermöglicht, so daß in der Übertragungsphase aus diesen schon vorher berechneten Informationen einfach und schnell Prüfsummen zu den gesendeten Signalen bzw. Daten berechnet werden können.

Die erfindungsgemäße Lösung ist im Kennzeichen des Patentanspruchs 1 charakterisiert.

Weitere Lösungen der Aufgabe bzw. Ausgestaltungen des Erfindungsgegenstandes sind in den kennzeichnenden Teilen der Patentansprüche 2 bis 10 charakterisiert.

Durch die bewußte Einführung einer Vorberechnungsphase und einer Kommunikationsphase in das Übertragungsverfahren ist es jetzt möglich, die Berechnung von Authentifikations-informationen schon vor der eigentlichen Übertragungsphase durchzuführen und während der Übertragungsphase können nun

aus diesen schon vorher berechneten Informationen einfach und schnell Prüfsummen zu den gesendeten Signalen berechnet werden. Die Lösung der Aufgabe besteht in einem Verfahren aus einer Vorberechnungsphase und einer Kommunikationsphase, in der die Signale bzw. Daten zusammen mit den Prüfsummen übertragen werden. In der Vorberechnungsphase werden mittels kryptographischer Algorithmen, zum Beispiel einer Blockchiffre im "Output-Feedback-Mode" aus dem Zeitvariantenparamenter (Sequenznummer, Zeitmarke und sonstigen Initialisierungsdaten) zunächst eine Pseudozufallsfolge Z erzeugt. Als Beispiel wird m = 16, 32 oder 64 für einen Sicherheitsparameter m angenommen. Aus der Folge Z werden jetzt sich nicht überschneidende Abschnitte z(i) von jeweils m Bit den Signalen s[i], i = 1, 2, ..., n des Signalvorrates zugeordnet. Aus der verbleibenden Folge werden weitere sich nicht überschneidende m Bit Abschnitte t[i] als Codierung der Nummern 1, 2, ... MAX gewählt, wobei MAX die maximale Anzahl der zu übertragenden Signale ist.

Wenn in der anschließenden Kommunikationsphase eine Senderauthentifikation erforderlich ist, wird zunächst dem Ablauf der "One pass authentication" gemäß den Veröffentlichungen ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication Mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994) und ISO/IEC 9798-4, Information technology - Security techniques - Entity authentication Mechanisms - Part 4: Mechanisms using a cryptographic check function (JTC1/SC27 1995) gefolgt. Der Sender überträgt die Initialisierungsformation und die zeitvarianten Parameter an den Empfänger und als Authentisierungstoken sendet er eine Anzahl bisher nicht verwendeter Bits aus Z an den Empfänger. Der Empfänger berechnet seinerseits die Pseudozufallsfolge Z und überprüft das empfangene Authentisierungstoken. Die während der Signalübertragung

vom Empfänger empfangenen Signale werden als authentisch akzeptiert, wenn die empfangenen Authentifikationstoken mit denen, die er berechnet hat, übereinstimmen. Darüberhinaus sind noch Modifikationen des Verfahrens möglich, die in der nachfolgenden Beschreibung noch im Einzelnen beschrieben werden.

Die Erfindung wird nun anhand von in der Zeichnung dargestellten Ausführungsbeispielen näher beschrieben. In der Zeichnung bedeuten:

Fig. 1 ein Flußdiagramm für die prinzipielle Operationsfolge im Empfänger und

Fig. 2 ein Flußdiagramm für die prinzipielle Operationsfolge in einem Sender.

Das Verfahren besteht aus einer Vorberechnungsphase und einer Kommunikationsphase, in der die Signale zusammen mit den Prüfsummen übertragen werden.

Vorbereitungsphase:
Mittels des kryptographischen Algorithmus (zum Beispiel einer Blockchiffre im "Output-Feedback-Mode" gemäß ISO/IEC 10116, Information Processing - Modes of Operation for an n-bit Block Cipher Algorithm (JTC1/SC27 1991)) wird aus einem zeitvarianten Parameter (Sequenznummer, Zeitmarke, gemäß ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication Mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994)) und sonstigen Initialisierungsdaten zunächst eine Pseudozufallsfolge Z erzeugt. Es sei m ein Sicherheitsparameter, zum Beispiel M = 16, 32 oder 64. Aus der Folge Z werden jetzt sich nicht überschneidende Abschnitte z[i] von jeweils m Bits den Signalen s[i], i = 1, 2, ..., n des Signalvorrates zugeordnet. Aus der

verbleibenden Folge werden weitere sich nicht überschneidende m Bit Abschnitte t[i] als Codierung der Nummern 1, 2, ...MAX gewählt, wobei MAX die maximale Anzahl der zu übertragenden Signale ist.

Kommunikationsphase:
a) Senderauthentifikation:
Falls eine Senderauthentifikation erforderlich ist, wird zunächst dem Ablauf der "One pass authentication" gemäß den Veröffentlichungen ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication Mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994) und ISO/IEC 9798-4, Information technology - Security techniques - Entity authentication Mechanisms - Part 4: Mechanisms using a crpytographic check function (JTC1/SC27 1995) gefolgt. Der Sender überträgt die Initialisierungsinformation und die zeitvarianten Parameter an den Empfänger. Als Authentisierungstoken sendet er eine Anzahl bisher nicht verwendeter Bits aus Z an den Empfänger. Der Empfänger berechnet seinerseits die Pseudozufallsfolge Z und prüft das empfangene Authentisierungstoken.

b) Signalübertragung und -authentifikation:
Sei s[k[1]] das erste Signal, das übertragen wird, dann sendet der Sender zur Authentifikation des ersten Signals T(1):=f(z[k[1]],t[1]), wobei f eine schnell berechenbare Verknüpfung der beiden Werte z[k[1]] und t[1] ist. Ein Beispiel für f ist die bitweise XOR Verknüpfung.

Für i = 2, 3, ..., i maximal MAX, sei s[k[i]] das i-te Signal, das übertragen wird. Zur Authentifikation dieses Signals sendet der Sender das Token T(i):=f(z[k[i]],t[i]). Der Empfänger führt jeweils dieselben Berechnungen aus und akzeptiert die empfangenen Signale als authentisch, wenn

die vom Sender empfangenen Authentifikationstoken mit denen, die er berechnet hat, übereinstimmen.

Die Reihenfolge der übertragenen Signale wird durch den Einfluß der Werte t[i] gesichert.

Eine Variante der Signalauthentifikation besteht im folgenden: Wenn es erforderlich ist, das Authentifikationstoken T(i) des i-ten Signals s[k[i-1]] abhängig von allen bisher gesendeten Signalen s[k[1]],...,s[k[i-1]] zu wählen, kann zur Authentifikation des i-ten Signals s[k[i]] das Token

T(i) = f(t[i], F(i)) gesendet werden, wobei
F(1) = s[k[1]] und
F(i) = f(s[k[i]],F(i-1)) für i > 1.

Die Berechnung des Authentifikationstokens T(i) erfordert somit zweimal die Berechnung von f.

Ein Beispiel für die Anwendung eines derartigen Verfahrens ist der authentische Verbindungsaufbau beim Telefonieren. Beim Senden der Wahltöne ist nicht bekannt, ob noch ein weiterer Wahlton folgt. Deshalb erscheint es erforderlich, jeden Wahlton in der ihm nachfolgenden Pause durch die Übertragung eines Tokens zu authentisieren. Beim Mehrfrequenzwahlverfahren beträgt die Länge der Wahltöne mindestens 65ms und die Pausenlänge zwischen den Wahltönen mindestens 80ms. Mit der Authentifikation, wie sie hier beschrieben ist, ist auch diese kurze Zeitdauer von 145ms zur Authentifikation ohne Probleme möglich.

Zunächst soll anhand des Flußdiagramms nach Fig. 1 die Operations- oder Schrittfolge des Empfängers beschrieben werden.

In dem Telefonbeispiel ist der Sender das Telefon, gegebenenfalls ausgestattet mit Kryptomodul und/oder

Chipkarte, und der Empfänger das Telefonnetz, zum Beispiel die nächste Vermittlungsstelle.

E1 und S1: Hier wird der zeitinvariante Parameter zwischen dem Empfänger und Sender synchronisiert. Der zeitinvariante Parameter kann eine Sequenznummer oder Zeitmarke sein, die synchronisiert vorliegt. Dieser Parameter darf gegebenenfalls auch zur Synchronisation im Klartext oder verschlüsselt vom Sender an den Empfänger gesendet werden. Im erfindungsgemäßen Verfahren ist es sinnvoll, daß der Sender den zeitinvarianten Parameter schon kennt, bevor ein Verbindungsaufbau gewünscht wird, um die s[], t[] vorzuberechnen.

E2 und S2: Hier berechnen Sender und Empfänger zunächst eine Zufallsfolge PRS (Pseudo-Random-Sequence) der Länge m*(smax+tmax) Bit, wobei

m: Sicherheitsparameter, im Beispiel m:=32.

smax: Maximale Anzahl der unterschiedlichen Signale (Anzahl der Elemente des Alphabets/Signalvorates). Im Telefon-beispiel die Ziffern 1..9 und Spezialsymbole wie #, und andere.

tmax: Maximale Anzahl der Signale, die in einem Durchgang authentisiert werden sollen. Im Telefonbeispiel max. Länge einer Telefonnummer, max. Anzahl von Ziffern und Spezialsymbolen für einen Verbindungsaufbau.

Danach werden jeweils sich nicht überschneidende Abschnitte von m Bits dieser Zufallsfolge PRS den m Bit Größen s[1], s[2], ..., s[smax], t[1], t[2], ..., t[tmax] zugewiesen:
s[1] = Bit 1 bis Bit m der PRS
s[2] = Bit m+1 bis Bit 2*m der PRS
...

s[max] = Bit (smax-1)*m+1 bis Bit smax*m der Zufallsfolge PRS

t[1] = Bit smax*m+1 bis Bit (smax+1)*m der Zufallsfolge PRS

...

t[tmax] = Bit (smax+tmax-1)*m+1 bis Bit (smax+tmax)*m der Zufallsfolge PRS

Anhand von Fig. 2 wird nachfolgend die Operations- oder Schrittfolge für den Sender beschrieben.

S3: Der Sender wartet auf ein Signal w, das authentisch übertragen werden soll. w wird als natürliche Zahl zwischen 1, 2, ..., smax interpretiert, um die Abbildung w -> s[w] einfach zu halten.

S4: Der Sender sendet das i-te Signal w zusammen mit dem Authentifizierungstoken f(s[w],t[i]). Im Telefonbeispiel ist das Token f(s[w],t[i])=s[w]+t[i], das bitweise XOR von s[w] und t[i].

S5: S3 und S4 werden solange iteriert wiederholt, bis entweder keine Signale mehr authentisch übertragen werden sollen oder die maximale Anzahl von Signalen, die mit diesem Vorrat an vorberechneter Zufallsfolge PRS authentisiert werden können, erreicht ist.

S6: Im Telefonbeispiel wartet der Sender jetzt auf den Verbindungsaufbau des Empfängers.

E3, E4 und E5: Solange neue Signale mit zugehörigen Authentisierungstoken empfangen werden, prüft der Empfänger, ob die von ihm berechneten Authentisierungstoken mit den empfangenen übereinstimmen.

E6: Falls alle Token übereinstimmen, werden die empfangenen Signale als authentisch akzeptiert. Im Telefonbeispiel erfolgt jetzt der Verbindungsaufbau.

E7: Bei nicht erfolgreicher Authentisierung erfolgt kein Verbindungsaufbau.

# P A T E N T A N S P R Ü C H E

1. Verfahren zum Übertragen von Signal-/Datenfolgen zwischen einem Sender und einem Empfänger mit Authentifizierung der übertragenen Signal-/Datenfolgen durch Verwendung von Schlüsseln und kryptographischen Algorithmen, die sowohl auf der Sender- als auch auf der Empfängerseite implementiert sind, dadurch gekennzeichnet,

   daß in einer Vorberechnungsphase mittels kryptographischer Algorithmen Daten abhängig von einem geheimen Schlüssel berechnet werden, aus denen in einer nachfolgenden Übertragungsphase Authentifikationstoken für die Signale berechnet werden, die sowohl die Signale als auch die Reihenfolge des Sendens der Signale authentisieren.

2. Verfahren nach Patentanspruch 1, dadurch gekennzeichnet,

   daß in der Vorbereitungsphase mittels eines kryptographischen Algorithmus eine Pseudozufallsfolge (PRS) erzeugt wird,

   daß aus dieser Folge bestimmte Abschnitte als Codierung sowohl der Signale des Signalvorrates als auch der Sendestellen (1, 2, ... MAX) verwendet werden und

   daß das Authentifikationstoken des Signals, das an i-ter (i = 1, 2, ..., MAX) Stelle gesendet wird, abhängig von der Codierung des Signals und von der Codierung der Sendestelle (i) berechnet wird.

3. Verfahren nach Patentanspruch 2, dadurch gekennzeichnet,

daß das Authentifikationstoken (T) des Signals, das an i-ter (i = 1, 2, ..., MAX) Stelle gesendet wird, die bitweise XOR-Verknüpfung oder eine äquivalente logische Funktion der Codierung des jeweiligen Signals und der Codierung der Sendestelle (i) ist.

4. Verfahren nach Patentanspruch 1, dadurch gekennzeichnet,

daß in der Vorberechnungsphase mittels eines kryptographischen Algorithmus eine Pseudozufallsfolge (PRS) erzeugt wird,

daß aus dieser Folge bestimmte Abschnitte als Codierung sowohl der Signale des Signalvorrates als auch der Sendestellen (1, 2, ..., MAX) verwendet werden und

daß das Authentifikationstoken des Signals, das an i-ter Stelle (i = 1, 2, ..., MAX) gesendet wird, abhängig von der Codierung aller bisher gesendeten Signale (1, 2, ..., i) und von der Codierung der Sendestelle (i) berechnet wird.

5. Verfahren nach einem der Patentansprüche 1 bis 4, dadurch gekennzeichnet,

daß das Authentifikationstoken (T) des Signals, das an i-ter Stelle (i = 1, 2, ... MAX) gesendet wird, die bitweise XOR-Verknüpfung oder eine äquivalente logische Verknüpfung der Codierung aller bisher gesendeten Signale (1, 2, ... i) und der Codierung der Sendestelle (i) ist.

6. Verfahren nach einem der Patentansprüche 1 bis 5, dadurch gekennzeichnet,

daß der in der Vorberechnungsphase verwendete kryptographische Algorithmus eine Blockchiffre ist.

7. Verfahren nach Patentanspruch 6, dadurch gekennzeichnet,

daß als Blockchiffre der bekannte "Data Encryption Standard" verwendet wird.

8. Verfahren nach einem der Patentansprüche 6 bzw. 7, dadurch gekennzeichnet,

daß die Pseudozufallsfolge (PSR) durch Betreiben der Blockchiffre im bekannten "Output-Feedback-Mode" erzeugt wird.

9. Verfahren nach dem Oberbegriff des Patentanspruchs 1 bzw. nach einem der Patentansprüche 2 bis 8, dadurch gekennzeichnet,

daß in der Vorbereitungsphase zusätzlich ein Token (T) zur Authentifikation des jeweiligen Senders berechnet wird, das nachfolgend übertragen wird und den Empfänger zur Authentifikation des Senders initiiert.

10. Verfahren nach einem der Patentansprüche 1 bis 9, dadurch gekennzeichnet,

daß die Reihenfolge der übertragenen Signale durch die sich nicht überschneidenden m Bit Abschnitte (t(i)) gesichert ist.

## Z U S A M M E N F A S S U N G

Das Verfahren zum Übertragen von Signal-/Datenfolgen von einem Sender zu einem Empfänger mit Authentifizierung der Signal-/Datenfolgen setzt sich aus einer Vorberechnungsphase und einer Kommunikationsphase zusammen, in der die Signale zusammen mit den Prüfsummen übertragen werden. In der Vorberechnungsphase wird mittels eines kryptographischen Algorithmus aus einem zeitvarianten Parameter und sonstigen Initialisierungsdaten zunächst eine Pseudozufallsfolge erzeugt. Aus einer Folge (z) werden sich nicht überschneidende Abschnitte (z(i)) von jeweils m Bits in Signalen (s(i)), i = 1, 2, ... n eines Signalvorrates zugeordnet. Aus der verbleibenden Folge werden weitere sich nicht überschneidende m Bit-Abschnitte (t(i)) als Codierung der Nummern (1, 2, ... MAX) gewählt. Der Sender überträgt die Initialisierungsinformation und die zeitvarianten Parameter an den Empfänger und der Empfänger berechnet seinerseits die Pseudozufallsfolge (Z) und prüft das empfangene Authentifikationstoken (T). Der Sender akzeptiert die empfangenen Signale als authentisch, wenn die vom Sender empfangenen Authentifikationstoken mit denen übereinstimmen, die er berechnet hat.

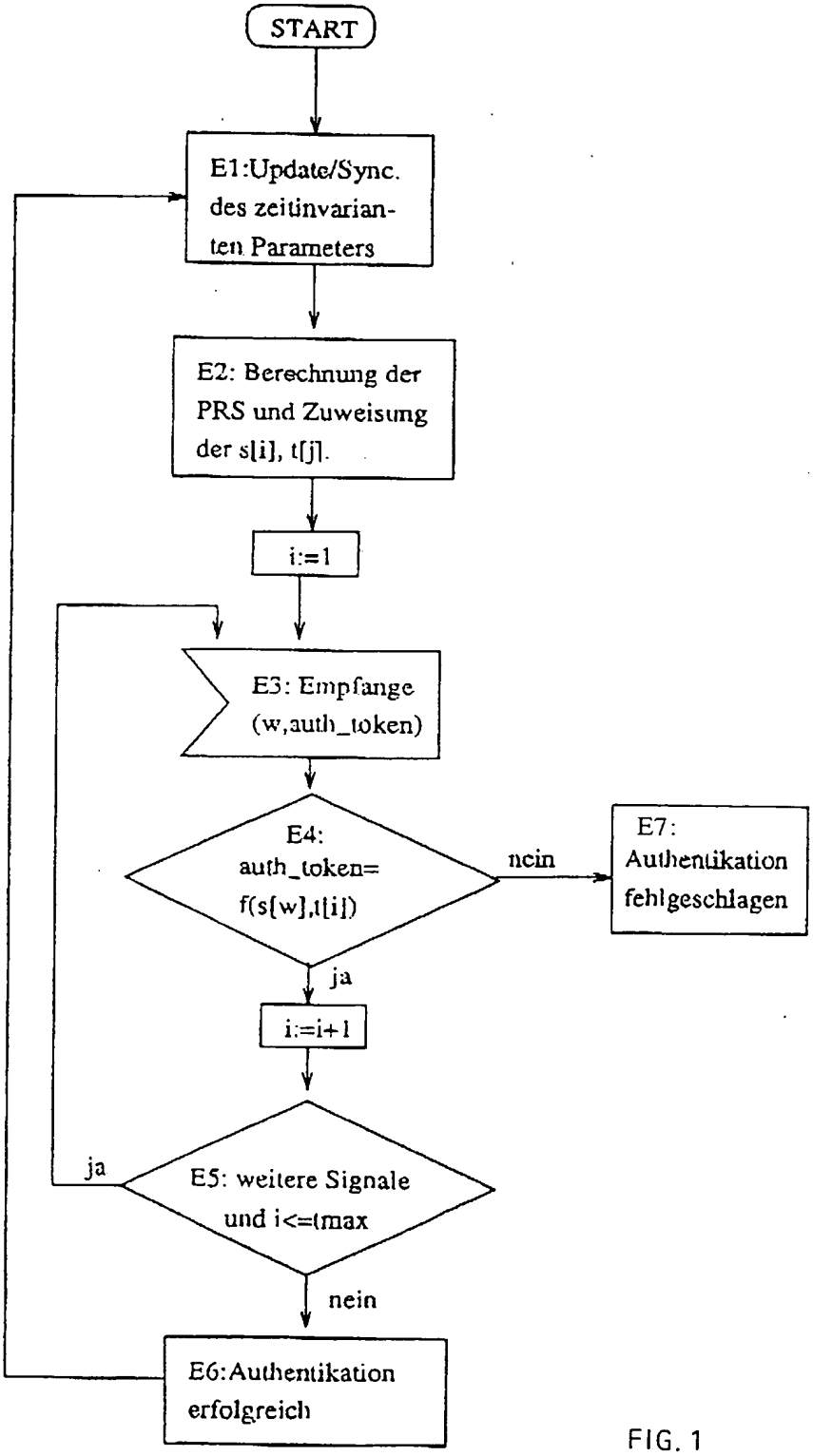
START
E1:Update/Sync. des zeitinvarianten Parameters
E2: Berechnung der PRS und Zuweisung der s[i], t[j].
i:=1
E3: Empfange (w,auth_token)
E4: auth_token= f(s[w],t[i])
nein
E7: Authentikation fehlgeschlagen
ja
i:=i+1
ja
E5: weitere Signale und i<=tmax
nein
E6:Authentikation erfolgreich

FIG. 1

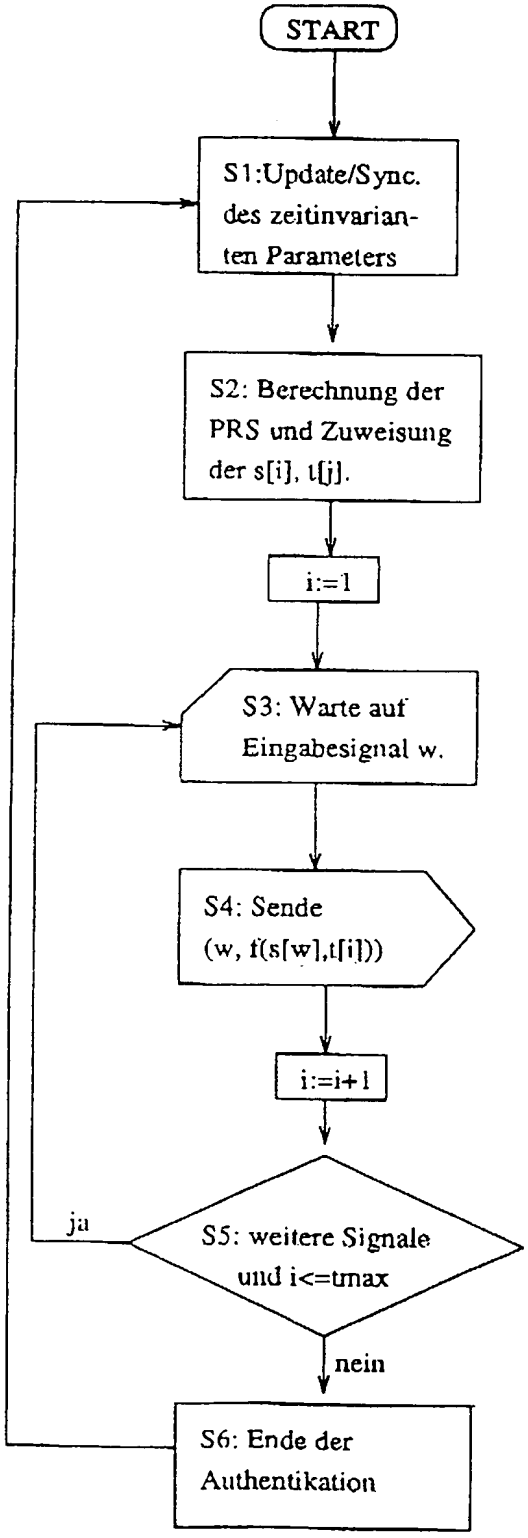
START
S1:Update/Sync. des zeitinvarianten Parameters
S2: Berechnung der PRS und Zuweisung der s[i], t[j].
i:=1
S3: Warte auf Eingabesignal w.
S4: Sende (w, f(s[w],t[i]))
i:=i+1
S5: weitere Signale und i<=tmax
ja
nein
S6: Ende der Authentikation

FIG. 2